This listing of claims replaces all prior versions, and listings of claims in the instant application:

Listing of Claims:

1.   (Currently amended) The method of Claim 22 wherein: A method comprising:

said decrypting said SMTP client application comprises emulating said a SMTP client application comprising generating at least one SMTP client application dirty page;

said decrypting said executable application comprises emulating an said executable application sent from said SMTP client application comprising generating at least one executable application dirty page; and

said determining whether said SMTP client application when decrypted is the same as said executable application when decrypted comprises determining whether said at least one SMTP client application dirty page is a match of said at least one executable application dirty page.

2.   (Currently amended) The method of Claim 1 22 further comprising establishing a SMTP proxy, wherein said SMTP client application forms a connection with said SMTP proxy.

3.   (Original) The method of Claim 1 further comprising determining whether SMTP client application dirty pages were generated during said emulating a SMTP client application, said SMTP client application dirty pages comprising said at least one SMTP client application dirty page.

4.   (Original) The method of Claim 3 further comprising saving a state of said SMTP client application upon a determination that said SMTP client application dirty pages were generated during said emulating a SMTP client application.

5.   (Currently amended)   The method of Claim ~~1~~22 wherein said SMTP client application sends data comprising said executable application.

6.   (Original)   The method of Claim 5 further comprising decomposing said data.

7.   (Original)   The method of Claim 5 further comprising determining whether said data comprises executable content.

8.   (Currently amended)   The method of Claim 5 ~~further comprising establishing a SMTP proxy,~~ wherein said data is intercepted and stalled by said SMTP proxy.

9.   (Original)   The method of Claim 5 further comprising stalling said data.

10.   (Currently amended)   The method of Claim ~~9~~1 wherein said SMTP client application sends data comprising said executable application, said method further comprising stalling said data, wherein upon a determination that said at least one SMTP client application dirty page is not a match of said at least one executable application dirty page, said method further comprising allowing said data to proceed.

11.   (Currently amended)   The method of Claim ~~9~~1 wherein said SMTP client application sends data comprising said executable application, said method further comprising stalling said data, wherein upon a determination that said at least one SMTP client application dirty page is a match of said at least one executable application dirty page, said method further comprising taking protective action to protect a computer system.

12.   (Original)   The method of Claim 11 further comprising determining that said match is not a known false positive prior to said taking protective action.

13.   (Original)   The method of Claim 11 further comprising providing a notification of said protective action.

14.   (Original)   The method of Claim 5 further comprising determining whether said data comprises executable applications that have not been emulated.

15.   (Original)   The method of Claim 14 wherein upon a determination that said data does comprised executable applications that have not been emulated, said method further comprising selecting a next executable application for emulation.

16.   (Original)   The method of Claim 15 further comprising emulating said next executable application.

17.   (Original)   The method of Claim 1 further comprising determining whether executable application dirty pages were generated during said emulating an executable application, said executable application dirty pages comprising said at least one executable application dirty page.

18.   (Currently amended)   The method of Claim ~~1~~ 22 wherein said SMTP client application is a polymorphic malicious code.

19.   (Currently amended)   <u>The method of Claim 22 wherein:</u> ~~A method comprising:~~

said decrypting said SMTP client application comprises
emulating a—said SMTP client application[[;]], said method
further comprising:

determining whether SMTP client application dirty pages
were generated during said emulating a—said SMTP client
application;

excluding said SMTP client application as a polymorphic
malicious code upon a determination that said SMTP client
application dirty pages were not generated; and

saving a state of said SMTP client application upon a
determination that said SMTP client application dirty pages
were generated.

20.   (Original)   The method of Claim 19 further
comprising:

stalling data from said SMTP client application;

determining whether said SMTP client application is
excluded as said polymorphic malicious code; and

allowing said data to proceed upon a determination that
said SMTP client application is excluded.

21.   (Currently amended)   A computer program product
comprising a polymorphic worm blocking application, said
polymorphic worm blocking application for:

establishing a SMTP proxy;

defining an application that forms a connection with said
SMTP proxy as a SMTP client application;

decrypting said SMTP client application comprising
emulating a said SMTP client application comprising generating
at least one SMTP client application dirty page;

intercepting an executable application sent from said SMTP
client application with said SMTP proxy;

decrypting said executable application comprising
emulating an said executable application sent from said SMTP

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

client application comprising generating at least one executable application dirty page; and

determining whether said SMTP client application when decrypted is the same as said executable application when decrypted comprising determining whether said at least one SMTP client application dirty page is a match of said at least one executable application dirty page.

22.   (Original) A method comprising:

establishing a SMTP proxy;

defining an application that forms a connection with said SMTP proxy as a SMTP client application;

decrypting said SMTP client application;

intercepting an executable application sent from said SMTP client application with said SMTP proxy;

decrypting said executable application; and

determining whether said SMTP client application when decrypted is the same as said executable application when decrypted.

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Page 8 of 10